REMARKS

In the Official Action mailed on **July 12, 2004,** the Examiner reviewed claims 1, 3-7, 9-13, 15-20, and 22-26. Claims 1, 3, 4, 5, 7, 9, 10, 11, 13, 14, 15, 16, 17, 19, 20, 22, 23, 24, and 26 were rejected under 35 U.S.C. §102(a) as being anticipated by Aziz (USPN 6,026,167, hereinafter "Aziz"). Claims 6, 12, 18, and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Aziz in further view of Tatebayashi et al (USPN 6,151,394, hereinafter "Tatebayashi").

Rejections under 35 U.S.C. §102(a) and 35 U.S.C. §103(a)

Independent claims 1, 7, 13, 19, 20, and 26 were rejected as being anticipated by Aziz. Applicant respectfully points out that Aziz teaches using **public-key cryptography and certificates** to establish a session key between nodes on a network (see Aziz, Abstract).

In constant, the present invention establishes a **table of pre-shared secret keys**, one for each potential user (see FIG. 3, index 312 of the instant application. The system then uses a negotiated secret key and a group secret key to encrypt the identity of a user, and then passes this **encrypted identity** to the firewall computer (see page 8. lines 20-21 and page 9, line 10 of the instant application). The firewall decrypts the encrypted identity and looks up the proper **pre-shared secret key** in the table of pre-shared secret keys (see page 9, lines 16-17 of the instant application). This technique is beneficial because it allows the establishment of encrypted communications between an external system and the firewall without the use of public-key cryptography and/or certificates. Public-key cryptography is a time-consuming process and the use of certificates requires a trusted certificate authority. The present invention eliminates the additional time needed for public-key cryptography and the need for a trusted certificate authority.

There is nothing within Aziz, either explicit or implicit, which suggests using a table of pre-shared secret keys, and using a negotiated secret key and a

group secret key to encrypt an identity of a user, subsequently decrypt the identity, and use the identity to look up a shared secret key for the user.

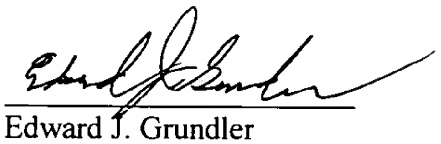
Accordingly, Applicant has amended independent claims 1, 7, 13, 19, 20, and 26 to clarify that the present invention establishes a table of pre-shared secret keys, uses a negotiated secret key and a group secret key to encrypt an identity of a user, subsequently decrypt the identity, and then use the identity to look up a shared secret key for the user. These amendments find support in FIG. 3, and on page 8, line 14 to page 11, line 10 of the instant application.

Hence, Applicant respectfully submits that independent claims 1, 7, 13, 19, 20, and 26 as presently amended are in condition for allowance. Applicant also submits that claims 3-6, which depend upon claim 1, claims 9-12, which depend upon claim 7, claims 15-18, which depend upon claim 13, and claims 22-25 which depend on claim 20 are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 

Edward J. Grundler
Registration No. 47, 615

Date: August 30, 2004

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
508 Second Street, Suite 201
Davis, CA 95616-4692
Tel: (530) 759-1663
FAX: (530) 759-1665